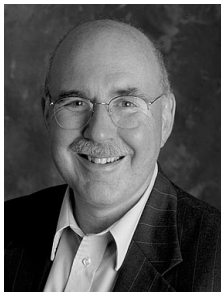
FORRESTER®

THE FORRESTER BRIEF



By Carl D. Howe

With Charles Rutstein

OCTOBER 26, 1999

Expiring Certificates Raise Y2K Specters

A glitch in the way sites guarantee Internet security on January 1, 2000, will spook consumers and add another hassle for Internet commerce SWAT teams. Firms should upgrade their digital certificates now to avoid losing online customers.

Every commerce site that offers secure transactions employs a digital certificate to provide encryption and reassure Web users that the site is authentic. But problems will appear in the New Year as:

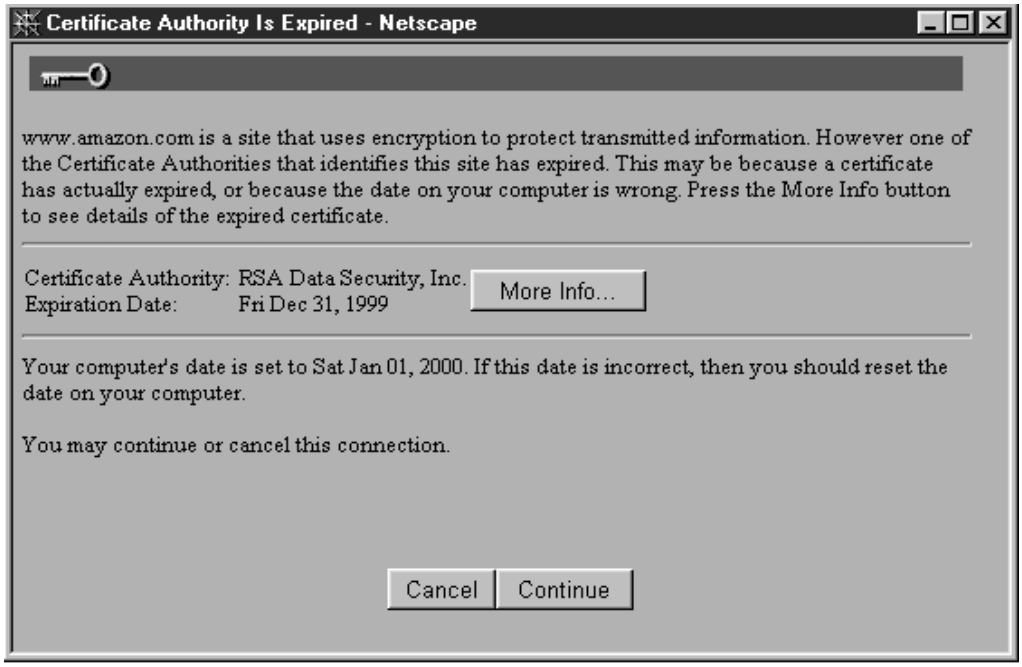
- **The root certificates for AT&T, CyberTrust, and VeriSign expire.** The certificates that these three issuers used to sign commerce site certificates for the last five years will expire on January 1, 2000. While all three companies have installed new root certificates and alerted commerce sites to the problem, thousands of certificates still must be replaced.
- **Users with old browsers get scary dialog boxes.** Even if sites renew their certificates prior to the New Year, visitors with Netscape browsers prior to Communicator 4.05 will continue to see confusing warning messages (see Figure 1). While users can still conduct transactions securely, they must upgrade their browsers to avoid receiving the warning on subsequent visits.

USERS WILL BLAME ONLINE SELLERS FOR EXPIRED CERTIFICATES

This isn't a big technical problem -- if users just click on the "continue" button, commerce sites will still encrypt and complete their transactions. But online companies must actively address the problem to prevent consumers from:

- **Flooding post-Christmas customer support lines.** After a banner $4 billion Internet Christmas season, retailers will still be struggling with gift returns when this expiration takes place (see the September 28, 1999 Forrester Brief "Online Merchants Must Brace For Holiday Shopping"). New Internet shoppers will phone customer support to complain or shop online elsewhere -- even though the retailer is blameless.

Figure 1 Browser Warnings About Expired Certs Will Scare Off Consumers



Source: Forrester Research, Inc.

- **Tarnishing the company with Y2K claims.** This certificate expiration couldn't happen at a worse time. On January 1, every consumer will be looking for Y2K mishaps, and broadcasters will plaster them on the national news as evidence of Y2K problems -- despite the fact that they have nothing to do with Y2K.

COMMERCE SITES SHOULD PUBLICIZE CERT EXPIRATION NOW

Forrester recommends that online retailers and brokers move aggressively to fix this problem by:

- **Replacing expiring certificates now.** If your company has an AT&T, CyberTrust, or VeriSign certificate, upgrade it today. Companies that feel burned by the bad timing of this expiration can purchase equivalent site certificates from certificate authorities such as Entrust, Equifax, or Thawte, whose certificates expire in 2010, not in 2000.

- **Encouraging users to upgrade their browsers.** CyberTrust, Entrust, and VeriSign all have Web pages that check whether a user's browser needs a certificate update and applies an appropriate patch. Copy the appropriate Web pages to your site; email your eCommerce customers the URL to bring them there; and add a money-saving coupon to encourage consumers to perform the update. Every consumer who updates now is one fewer customer who will complain on New Year's Day -- and one less hassle to deal with after Y2K.
- **Putting the problem in context.** Secure sites should note the efforts they are making to keep user data secure. Emphasize that this is not a Y2K problem -- on the Web site, in press releases, and in print advertising -- to keep Y2K ambulance chasers at bay.

FOR MORE INFORMATION

Information on what to do about root certificate expirations can be found at the following locations:

http://www.cybertrust.com/cybertrust/resources/root/expiration.html

http://www.equifaxsecure.com/servercert/faq.html

http://www.entrust.net/learning/rootca.htm

For instructions on how to upgrade Netscape browsers to recognize new root certificates, go to:

http://verisign.netscape.com/security/rootcert